GIGABYTE
TECHNOLOGY

54Mbs Wireless PCI Adapter
GN-WP01GS

User's Manual

http://www.gigabyte.com.tw

Version 1.0

Federal Communication Commission Interference Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:
To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Contents

CHAPTER 1 PRODUCT OVERVIEW 1

1.1 INTRODUCTION TO THE GN-WP01GS WIRELESS PCI ADAPTER 1
1.2 FEATURES 1
1.3 PHYSICAL DIMENSIONS & PACKAGING 2
1.4 LED INDICATOR 2
1.5 SYSTEM REQUIREMENTS 2

CHAPTER 2 INSTALLATION 3

2-1. INSTALLING THE ADAPTER (HARDWARE INSTALLATION) 3
2-2. INSTALLING THE DRIVER & UTILITY 4
2-3. SMARTSETUP 3 7

CHAPTER 3 USING THE WIRELESS UTILITY 9

3.1. PROFILE TAB 9
3.2. LINK STATUS TAB 17
3.3. SITE SURVEY TAB 18
3.4. STATISTICS TAB 19
3.5. ABOUT TAB 20

APPENDIX A TROUBLESHOOTING 21

APPENDIX B SPECIFICATIONS 22

APPENDIX C REGULATORY INFORMATION 23

APPENDIX D WARRANTY 24

Chapter 1 Product Overview

1.1 Introduction to the GN-WP01GS Wireless PCI Adapter

The Gigabyte WP01GS Wireless PCI Adapter installs quickly into your motherboard's PCI slot, connecting wirelessly to your Wi-Fi Router - instantly transforming your PC into a wireless AP, broadening the range of your wireless network.

The WP01GS is fully 802.11b interoperable, meaning it connects seamlessly to both 11b and 11g wireless traffic, and with its dynamic speed adjustment feature, it will always connect at the highest possible speed – up to 54Mbps.

The Gigabyte WP01GS Wireless G PCI Adapter makes connecting to a wireless router or access point a cinch with its included WLAN software utility – SoftAP™ – that automatically detects and lists all available wireless networks. Since the WP01GS can be setup in Wireless Distribution System (WDS), it transforms your desktop into an wireless access point, effectively expanding the range of your wireless network.

Secure
With its support for the highest level of encryption common today - 128 bit WEP, 802.1X, WPA and WPA2 - the WP01GS is perfect for the home user, keeping your data secure.

Robust
Move huge files and digital video blazingly fast! Up to 5 times faster than the common 11b solution. The high gain antenna and 802.11g wireless standard gives you continuous access to your home wireless router or office network,

Convenient
Saves the time and expense of installing Ethernet cabling when you want to set up or expand a network, and makes it simple to relocate your desktop PC.

1.2 Features

- Conforms to IEEE 802.11b and 802.11g specifications.
- Wireless transmits data rate up to the maximum speed of 54Mbps.
- Support 64-bit /128-bit WEP encryption, TKIP, 802.11i, WPA and WPA2.
- Provide Quality of Service (QoS) 802.11e, WMM.
- Supply international regulation 802.11d + h.
- Cisco CCX v1.0, v2.0, v3.0 compliance
- Dynamically scales the data rate.
- Automatic power management to reduce battery consumption.
- Seamless roaming between 802.11b and 802.11g networks.
- Driver supports Windows 98SE/Me/2000/XP.

1.3 Physical Dimensions & Packaging

Dimensions: 134mm × 121mm × 22mm

Before beginning the installation procedures, please inspect the components to assure that they have not been damaged during shipping. The components include:

Package Contents

- GN-WP01GS PCI Adapter
- Low profile external antenna
- Setup CD
- Quick Start Guide

In case of any missing or damaged accessories, please contact your local distributor or authorized reseller immediately. If you require returning the damaged product, you must pack it in the original packing material or the warranty will be voided.

1.4 LED Indicator

The WP01GS PCI Adapter has two LED lights located on the outward facing bracket frame. The left LED is the Activity LED and the right LED is the Link LED. Description follows.

ACT	OFF	ON	ON
LINK	OFF	ON	BLINK
Meaning	Network card is not functioning	Network card is connecting to network	Network card is sending/receiving data.

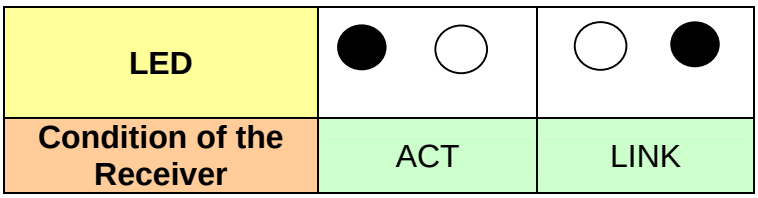

Figure 1 – Adapter LED

1.5 System Requirements

For trouble free installation and operation, please assure your PC meets the following minimum system requirements:

- Notebook or Desktop PC with a Pentium® 300 MHz or higher compatible processor with an available PCI slot.
- A CD-ROM drive.
- 20 Mbytes of free hard disk space.

Chapter 2 Installation

This chapter covers the installation of the WP01GS Adapter for your desktop PC. The following sections will assist you with proper installation of the PCI Adapter, and also with installing the necessary drivers and utilities. For specific information regarding your Version of Windows, please refer to the appropriate sections as indicated

2-1. Installing the Adapter (Hardware Installation)

Step 1: Power off your PC.

Step 2: Plug the PCI Adapter into an open PCI slot on the motherboard by pressing the card gently until the card edge connecter is completely and firmly inserted into your motherboards PCI slot.

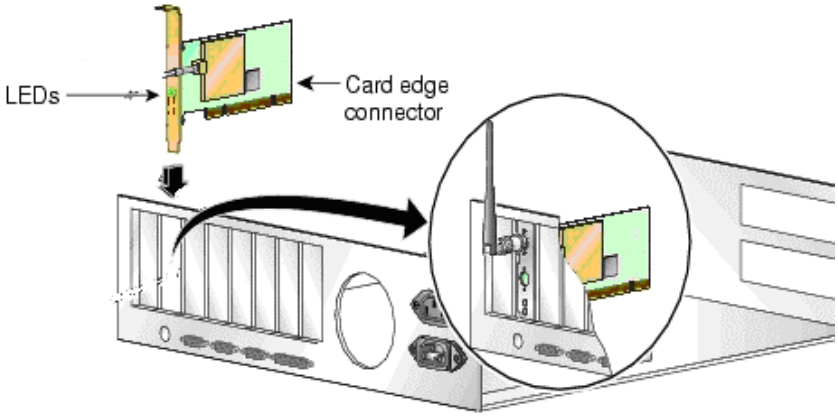

Figure 2. Insert your PCI Adapter

Step 3: Once inserted, attach the antenna on the mount of the PCI Adapter by screwing it on clockwise as shown in the figure below.

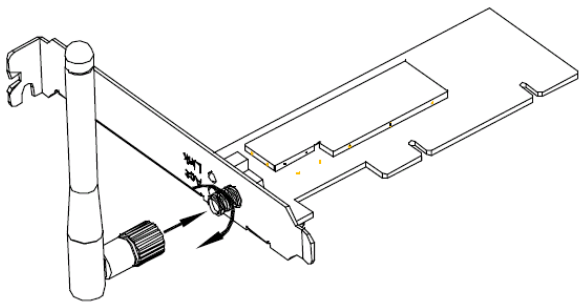

Figure 3. Attach the high gain antenna

Step 4: Power on your PC.

2-2. Installing the Driver & Utility

After restarting your computer the Windows **Found New Hardware** wizard will open. When it does, please click **Cancel** to close it. GIGABYTE drivers and utilities offer more power and control over your new WP01GS PCI Adapter than does Windows native Zero Configuration Utility.

Step 1: At the Found New Hardware Wizard screen, click **Cancel**.

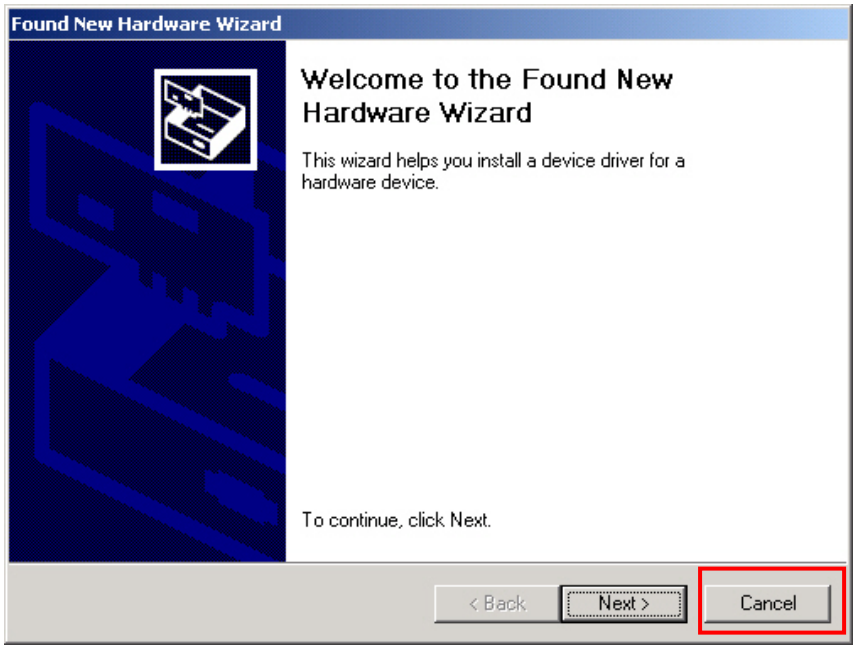
Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install a device driver for a hardware device.
To continue, click Next.
< Back
Next >
Cancel

Figure 4. Found New Hardware Screen

Step 2: Insert the WP01GS Setup CD into the CD-ROM drive. The WP01GS Welcome screen window will automatically open.

Step 3: From the main menu, click **"Install Wireless LAN Utility"**.

Figure 5. WP01GS Welcome Screen

Step 4: InstallShield will install the WP01GS drivers. Click **Next** to proceed.

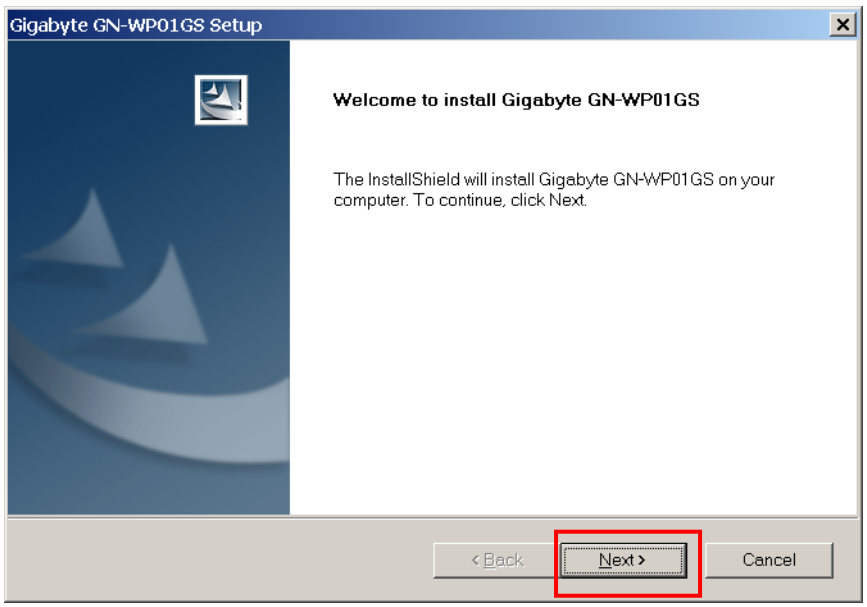
Gigabyte GN-WP01GS Setup
Welcome to install Gigabyte GN-WP01GS
The InstallShield will install Gigabyte GN-WP01GS on your computer. To continue, click Next.
< Back
Next >
Cancel

Figure 6. InstallShield

Step 5: Setup will detect your version of Windows. Click **Next**.

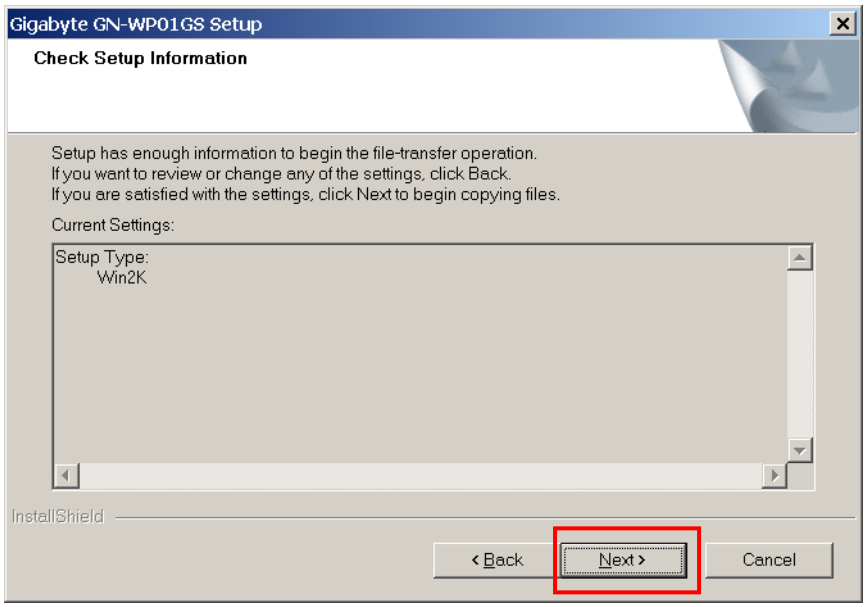
Gigabyte GN-WP01GS Setup
Check Setup Information
Setup has enough information to begin the file-transfer operation.
If you want to review or change any of the settings, click Back.
If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Setup Type:
Win2K
InstallShield
< Back
Next >
Cancel

Figure 7. InstallShield Detect Windows OS

Step 6: Since your card is already inserted, Click **OK**.

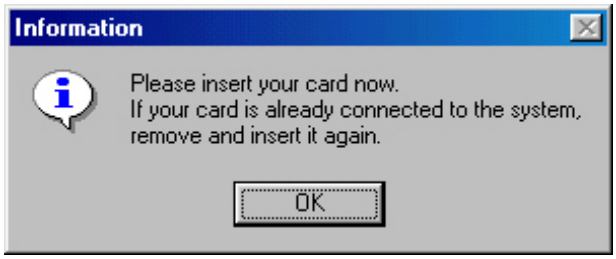

Figure 8. Windows Logo Testing

Step 7: Click **Finish** to complete installation.

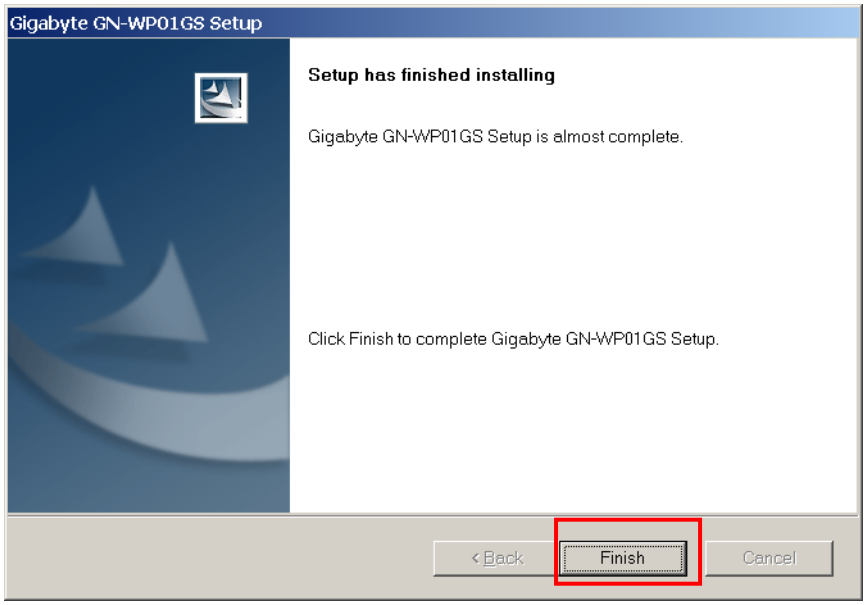

Figure 9. InstallShield Complete

2-3. SmartSetup 3

Note: The following section applies to users of GIGABYTE Wireless Routers.

GIGABYTE SmartSetup 3 is a powerful, yet user-friendly wireless network configuration wizard specially designed for GIGABYTE wireless networks. If you are connecting to a GIGABYTE wireless router, SmartSetup 3 will detect this and activate.

In three easy steps, you can establish a bulletproof WPA wireless network AND configure your Internet connection. Only GIGABYTE delivers this easy, powerful and secure solution for your wireless network!

Step 1: Select the GIGABYTE wireless router from the available networks.

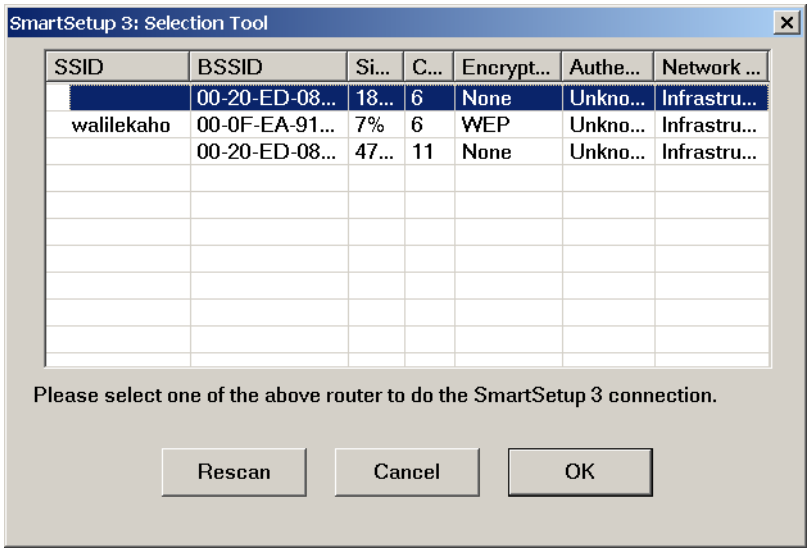

Figure 10. SmartSetup 3 Network Selection

Step 2: Create a WPA Passphrase using any keyboard character. Make it no less than 8 but no more than 63 characters in length. Anyone wishing to gain access to your network, will first need to key-in this Passphrase. In the example below, we used 'I love green eggs and ham'.

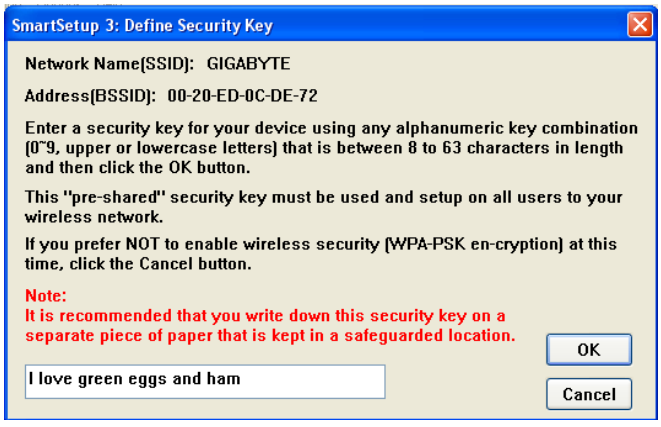
SmartSetup 3: Define Security Key
Network Name(SSID): GIGABYTE
Address(BSSID): 00-20-ED-0C-DE-72
Enter a security key for your device using any alphanumeric key combination (0~9, upper or lowercase letters) that is between 8 to 63 characters in length and then click the OK button.
This "pre-shared" security key must be used and setup on all users to your wireless network.
If you prefer NOT to enable wireless security (WPA-PSK en-cryption) at this time, click the Cancel button.
Note:
It is recommended that you write down this security key on a separate piece of paper that is kept in a safeguarded location.
I love green eggs and ham
OK
Cancel

Figure 11. SmartSetup 3 Define Passphrase

Step 3: Your GIGABYTE router's web configuration utility will automatically open, and detect your ISP type. Just key in the Username and Password. **Done.**

Figure 12. Auto detecting your ISP type

Note: *If Figure 12 does not appear, please type 192.168.1.254 in the address bar of your web browser, and click "Smart Setup" from the main menu which displays. For more information about SmartSetup 3, please see the enclosed Quick Start Guide.*

Congratulations. Your secure WPA wireless LAN and Internet

Chapter 3 Using the Wireless Utility

The WP01GS Wireless Utility is a powerful application that helps you to configure the network card and monitor the statistics of the communication link. This application permits the configuration for parameters while the card is operating. It also offers more configuration options and supports Windows 98SE/Me/2000/XP. Switch between AP mode and Station mode with just a right click of the mouse on the icon (Windows XP/2000 users only).
It appears as an icon in the task bar at the bottom right corner of screen whenever the card is operating *(see **Figure 13**)*. The quick start icon also doubles as a signal strength monitor, as indicated by its four small green lights.

Figure 13. WP01GS Utility quick start icon

To open the WP01GS Utility, either double click the quick start icon located in your system tray, or from the Windows **Start** menu, select **Programs, GIGA-BYTE 802.11 WLAN, GN-WP01GS SoftAP** and then **GN-WP01GS Utility**.

Note: *You may only use the utility to change wireless configurations when the WP01GS Adapter is enabled and operating. You have to use Windows native Zero Configuration tool provided with Windows when the Adapter is not enabled.*

3.1. Profile Tab

The **Profile** tab shows you the current association information about the profile. *(*see ***Figure 14****)*. Profiles are useful if you often associate with different access points. You can configure a group of settings depending on the access point you often associate with. and save as a profile, Click the **Add** button to create a new profile (see section below for further details), the Delete button to delete a selected profile, the **Edit** button to modify a selected profile and click the **Activate** button to have a selected profile become active.

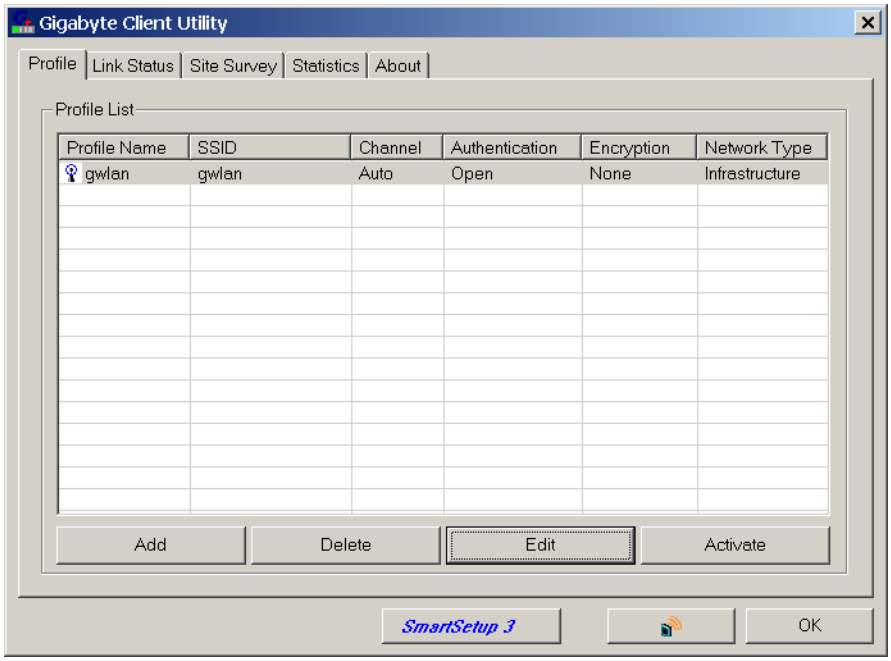

Figure 14. Current profile

Description of items in ***Figure 14*** is as follows:

Profile Name: A profile can be saved for various wireless settings in different environments, i.e. home, office, and the corner coffee shop.

SSID: Displays the SSID of the Adapter or Access Point.

Channel: Shows the current wireless channel.

Authentication: Sever authentication types. They include “OPEN”, “WPA”, “WPA-PSK” and “Shared”.

Encryption: The type of encryption used in this profile: “None”, “WEP”, “AES” and “TKIP”.

Network Type: Informs you if an Access Point (infrastructure) or other access points (802.11 Ad Hoc) are connected. In 802.11 Ad Hoc, you may select a channel for all members in 802.11 Ad Hoc.

3-1-1. Configuration Screen

You may **ADD** new profiles, or **EDIT** existing ones. *(see **Figure 15**)*

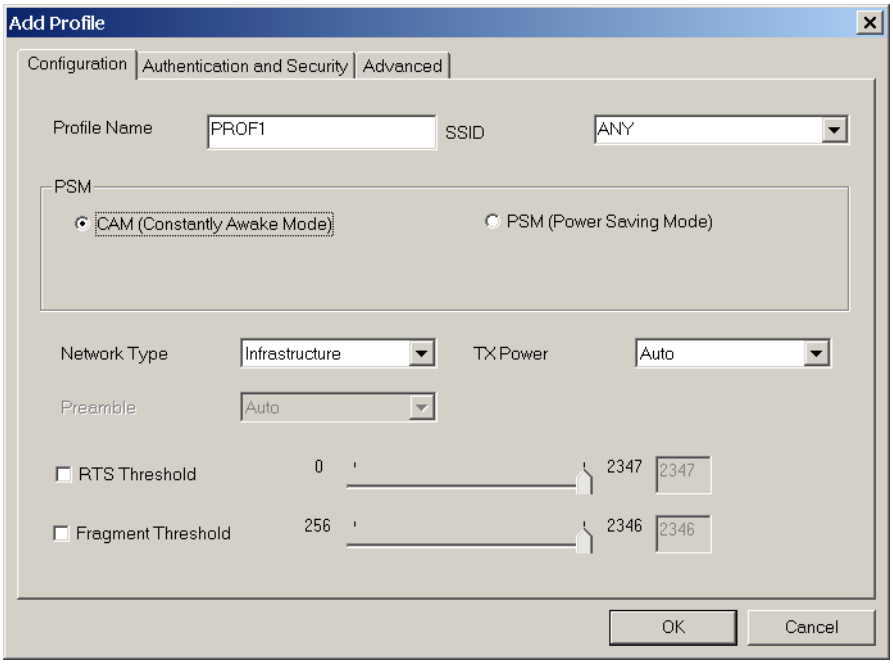

Figure 15. Configuration Screen

Description of items in ***Figure 15*** is as follows:

Profile Name: Users can save different profiles names for different configurations.

SSID: Select the AP detected by the system from the drop-down menu or input a SSID. (Default: ANY)

Power Saving mode: Select “Power Saving Mode” (PSM) to turn off the Adapter’s transceiver when not in use, or select CAM to continuously turn on transceivers. (Default: OFF)

Network Type: “Infrastructure” and “802.11 Ad Hoc”. When Infrastructure network type is chosen, PSM will function but not Preamble. On the contrary, when Ad hoc type is chosen (see ***Figure 15***), Preamble will function but not PSM. Also, the Channel option will appear and 802.1X Authentication will be disabled. (Default: Infrastructure)

TX Power: Select percentage of transmitted power. (Default: Auto)

RTS Threshold: This is a mechanism implemented to prevent the “Hidden Node” problem, “Hidden Note” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other and can not detect each other. This mechanism is a way to prevent data collision when Adapters require transmission. (Default: OFF)

Fragment Threshold: Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. (Default: OFF)

3-1-2. Authentication and Security Screen:

If an authentication or security setting is configured in your Access Point or router, you must enable this function to ensure successful connection. Use the following tab to configure data security and ID authentication (see ***Figure 16***). You may configure different settings in the profile, including 802.11 Protocol Authentication and Security and 802.1X Protocol.

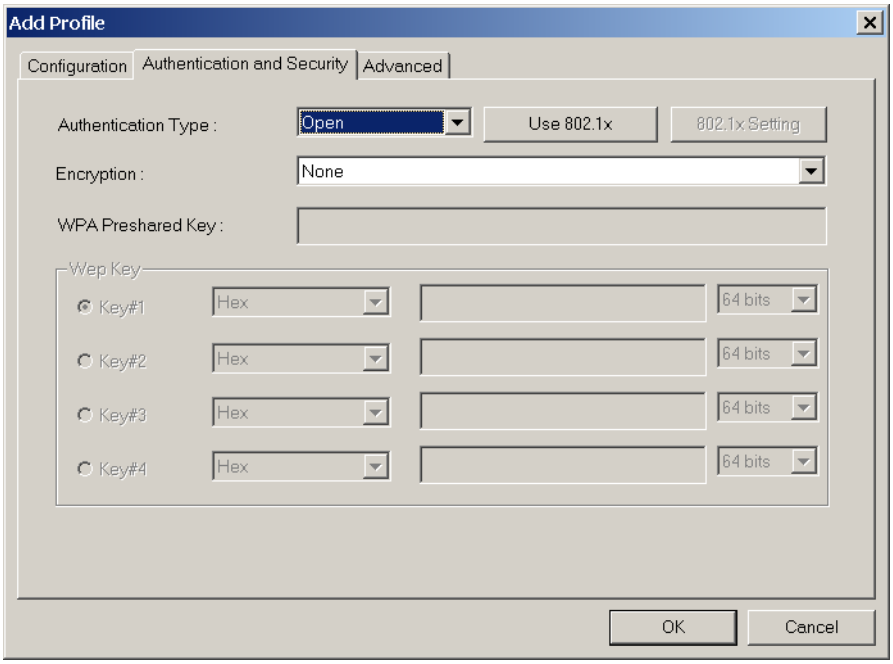

Figure 16. Authentication and Security

Authentication: Before a station connects to a SSID, the authentication type used by the SSID must be known. Authentication types include OPEN SYSTEM, SHARED, LEAP, WAP, WAP-PSK, WPA2 and WPA2-PSK. (Default: Open)

Encryption: To prevent unauthorized access to data transmitted on the network, the Adapter and the Access Point agree on a type of data encryption. Any station that wishes to connect, must have the same password and encryption scheme to connect. Different authentication types have different level of security.

WEP encryption: Select one of the four keys as the default encrypted key.

To setup WEP, you will need to set a ASCII or HEX key to connect to Access Point. The WEP Key can only be saved through the setting of profile.

1. Select a Key #.
2. Select a form of the key (Hex or ASCII).
3. Enter password. Please enter 26 hexadecimal digits or 13 ASCII digits.
4. Click OK to save the settings.

Making HEX keys:

64-bit - Generated as 10 alphanumeric characters (0-9, a-f) (example: 843c29a562)
128bit - Generated as 26 alphanumeric characters (0-9, a-f) (example: 3c29f2536bef3276d32e364a2c)

Note: *Using a Hex key is more secure than using an ASCII key, and if you are connecting to a GIGABYTE Router or Access Point, ASCII keys are not allowed and you must use a Hex key.*

WPA/WPA2-PSK encryption: WPA/WPA2-PSK (Preshared Key) uses TKIP or AES based on your choice. You create a password (or Passphrase as its often called) and the system will use the Passphrase to create a cipher code in which it will encrypt the data.

To use WPA/WPA2-PSK:

1. Create a Passphrase, and key it in. Use 8~63 ASCII digits.
2. Remember this Passphrase. If you forget the Passphrase, you will have to do a hard reset of the Access Point in order to restore default settings and connect again.
3. Click “OK to save these settings.

3-1-2-1. 802.1X Setting - Certification Tab

Clicking **Use 802.1X Authentication** and then **Enter 802.1X configuration** from the Authentication and Security Window will bring up the 802.1x Setting Window and the **Certification Tab (***see* ***Figure 17).***

From the Certification screen, you may configure information about authentication, such as Tunnel Protocol, ID and Password and Client Certificate or Certificate Chain. *(see* ***Figure 17 and 19****)*

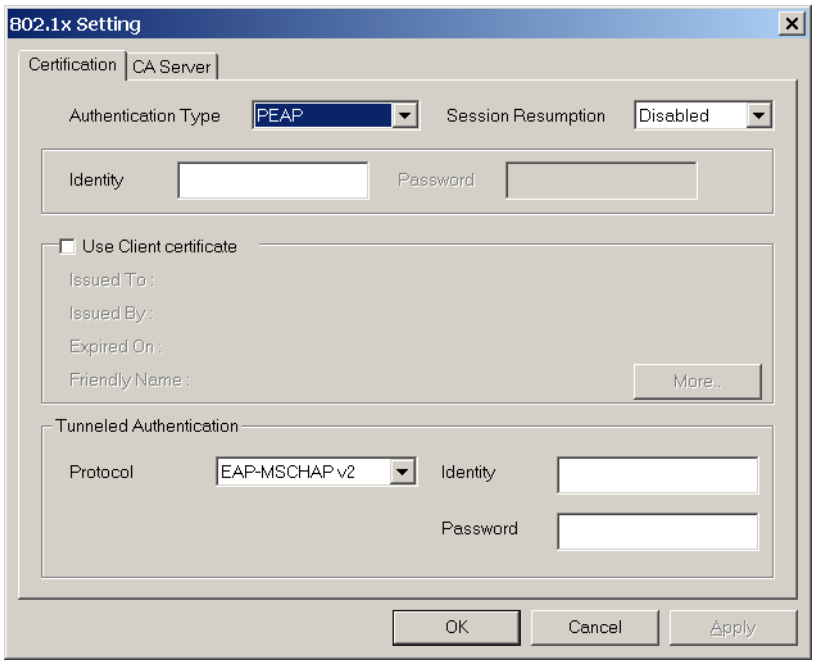

Figure 17. 802.1X Authentication

Description of items in ***Figure 17*** is as follows:

Authentication type: PEAP, TLS/Smart Card, TTLS and MD5-Challenge. (Default: PEAP)

Session Resumption: This feature can create a new connection without the overhead of

a full handshake.

Identity: The Account's User ID.

Password: Passwords for users accounts can be used when LEAP and MD5-Challenge are selected as authentication types.

Use Client Certificate: This certificate is necessary for TLS and an option for PEPA and TTLS. Check "Use Client Certificate" to verify the authenticity of a Client Certificate during the authentication process.

Clicking **More** will open the **Client Certificate Selection** Window (shown in ***Figure 18***). Users can select one suitable certificate as Client Certificate. (Default: OFF)

Tunnel Authentication: PEPA and TTLS use two-step authentication method. The first step is that Server sets up a Tunnel with its authentication. No option is need to be set for Client (the PC with the Adapter). The second step is to confirm the validity of Client with assigned authentication type in the Tunnel. Data needed for authentication includes Tunnel ID, Tunnel Password, Client Certificate or Server Authentication.

Protocol: Use assigned authentication type in the safe tunnel.

Tunnel ID: Users' accounts.

Password: Passwords for users' accounts.

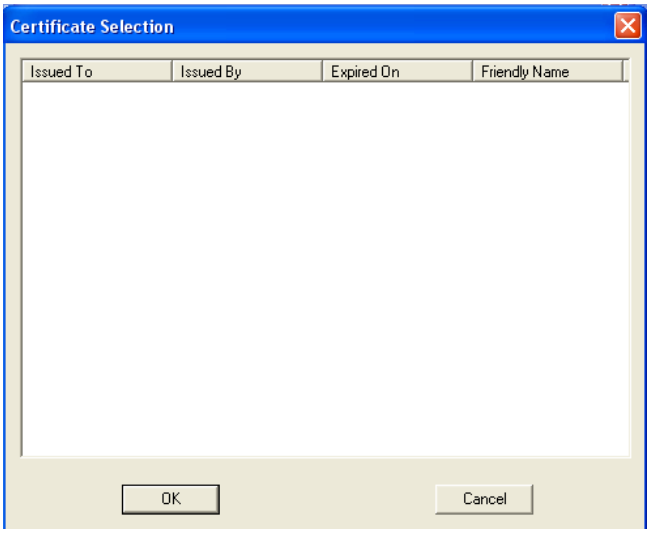

Figure 18. Client Certificate Selection List

3-1-2-2. 802.1x Settings - CA Server Tab

CA Server is used when TLS, TTLS or PEAP is in use. When **Use certificate chain** is checked, the Client can verify if such server is reliable and then transmit Client Certificate after the verification is confirmed.

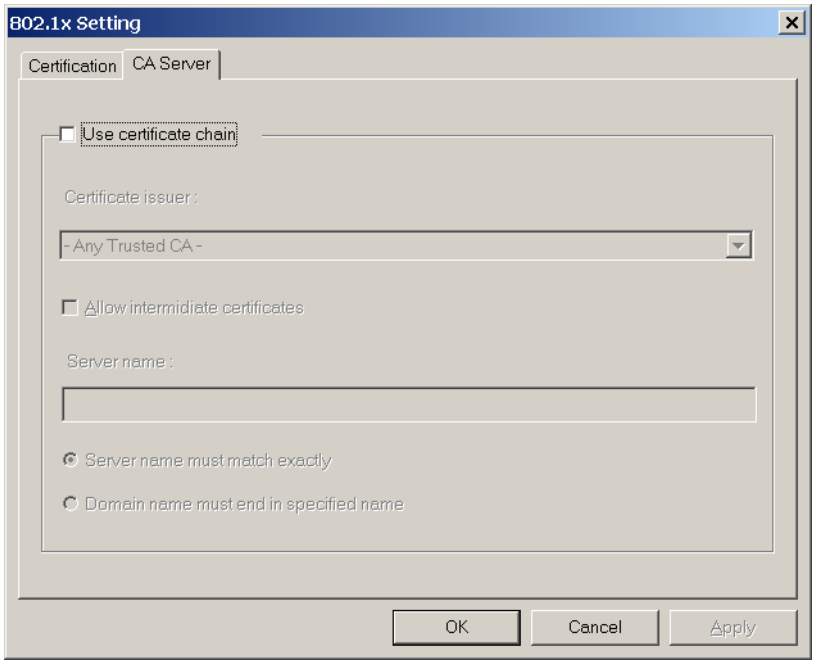

Figure 19. CA Server Setting

To verify the CA server:

1. Confirm if the Server Certificate is issued by assigned certificate issuer. If “Allow Intermediate Authentication” is checked, the server certificate can be issued by one intermediate certificate issuer.

2. Check the server name of server certificate is the same as the name entered by the user or belongs to the same domain.

Use certificate chain: If “Use certificate chain” is checked, it indicates that Client will confirm whether CA server is reliable. (Default: OFF)

Certificate issuer: CA of a server certificate can be selected from certificate issuers on the drop-down list. (Default: ANY)

Allow intermediate Certificates: When this option is checked, the certificate issuer can be an issuer recognized by a specific certificate issuer. On the other hand, the server certificate must be issued by a certificate issuer selected by the user.

Server name: This value can be a server name or the name of a domain where the server is located.

Server name must match exactly: If this option is selected, the server name of server certificate must be the same as “Server Name” or as the name of domain where the server is located.

Domain name must end in specified name: If this option is selected, the certificate issuer must be the domain or secondary domain entered in “Server Name”.

3-1-3. Advanced Screen

The **Advanced** screen includes fields of various parameters to review or change drivers. Just click OK to apply any changes in parameters in the tab. A reboot is **not** needed for changes to take effect. *(see **Figure 20**)*

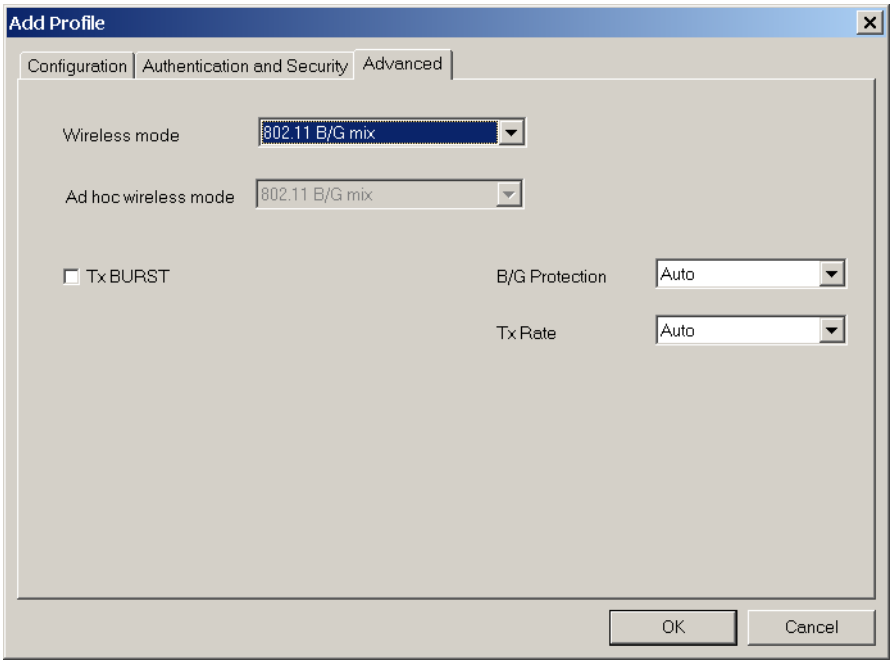

Figure 20. Advanced Screen

Description of items in ***Figure 20*** is as follows:

Wireless Mode: Sets infrastructure Protocols, including 802.11 B/G mix and 802.11 B Only. (Default: 802.11 B/G mix)

Ad Hoc Wireless Mode: Sets Ad Hoc Wireless Protocols, including 802.11 B/G mix, 802.11 B Only and 802.11 G Only. (Default: 802.11 B/G mix)

TX Burst: The longest interval between frames is normally one DIFS while frames are transmitted. When this setting is open, the longest interval between frames is one SIFS that means the system is allowed to transmit higher capacity of data in one interval. (Default: OFF)

B/G Protection: 802.11b uses CCK modulation. 802.11g uses OFDM while CCK modulation for 802.11b is compatible. To prevent data collision between two stations with 802.11b and 802.11g within range of the same Access Point, it is necessary to set 11B/G Protection. This setting only functions when 802.11 B/G mix is selected as Wireless Mode. Three setting are available: AUTO, ENABLE and DISABLE.

This is a mechanism implemented to prevent the “Hidden Node” problem, “Hidden Node” is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other and can not detect each other. This mechanism is a way to prevent data collision when WLAN equipments require transmission.

TX Rate: This option adjusts settings of TX Rate according to the setting of “Infrastructure Wireless Mode”. (Default: Auto)

3.2. Link Status Tab

The **Link Status** tab displays the current association information about the Adapters connection with a wireless network. *(see **Figure 21**)*

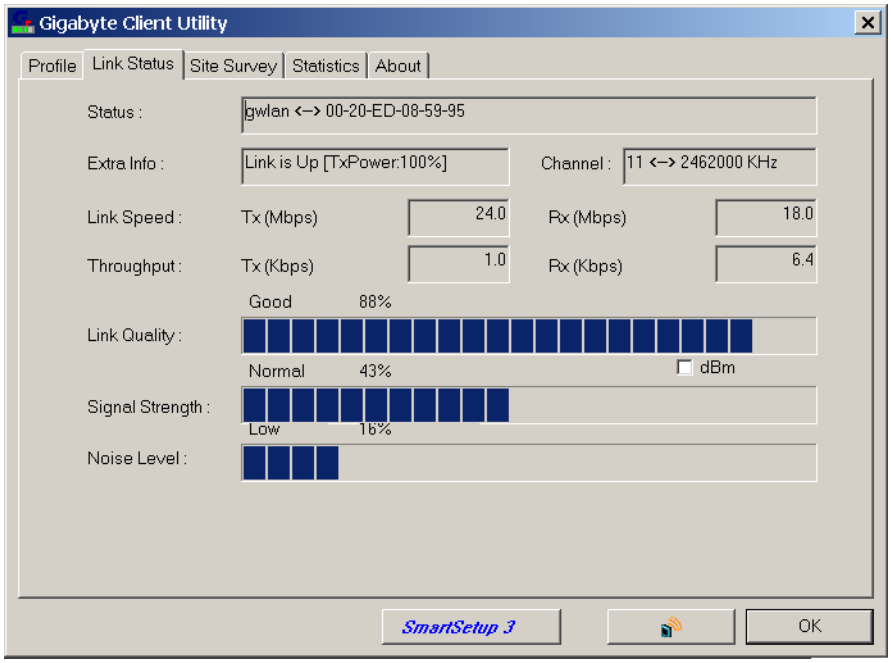

Figure 21. Link Status

Description of items in ***Figure 21*** is as follows:

Status: Shows current link status. “No Link” will appear on the screen when no connection is available. Otherwise, SSID and BSSID of a link will appear.

Extra Info: Show current link extra information.

Channel: The current channel number used by the Adapter.

Link Speed: Transmission rate (transferring and receiving) at which data is transferred between Stations with Adapter and AP. The speed will adjust according to different modes (802.11b, 11g or mixed) and distance.

Throughput: displays the transmitting (Tx) and receiving (Rx) bytes per second.

Link Quality: Measures quality of the link according to the quality of received AP signal.

Signal Strength: Measures signal strength received by RF signal processor and displays the signal strength in dBm.

Noise Level: Noise level during connection.

3.3. Site Survey Tab

The **Site Survey** tab shows you the list of reachable access points and/or peer-to-peer Stations. Just double click on the SSID that you want to connect or click the **Connect** button. *(see **Figure 22**)*

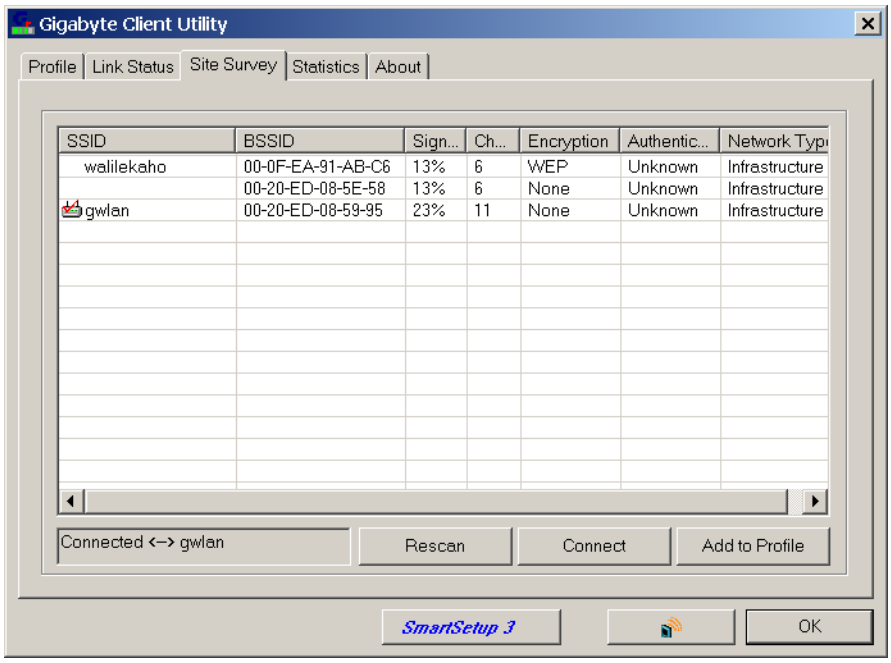

Figure 22. Site Survey

Description of items in ***Figure 22*** is as follows:

SSID: The name of the wireless network (also known as Network Name).

BSSID: Displays the MAC address of the Access Point or router.

Signal Strength: Displays the strength of the signal from a station to the AP.

Channel: Displays the current channel number used by the Access Point.

Encryption: The security method used by the Access Point.

Authentication: The authentication type used by the Access Point.

Network Type: Informs you if an Access Point (infrastructure) or other stations (802.11 Ad Hoc) is connected. When it is 802.11 Ad Hoc, we can select a channel for all members in 802.11 Ad Hoc.

Rescan: Rescan the available networks and then re-display results.

Connect: Connects with the highlighted Access Point.

Add to Profile: Adds a specific Access Point into the profile.

3.4. Statistics Tab

The **Statistics** tab shows you the number of packets sent and received by the Adapter *(see **Figure 23**)*

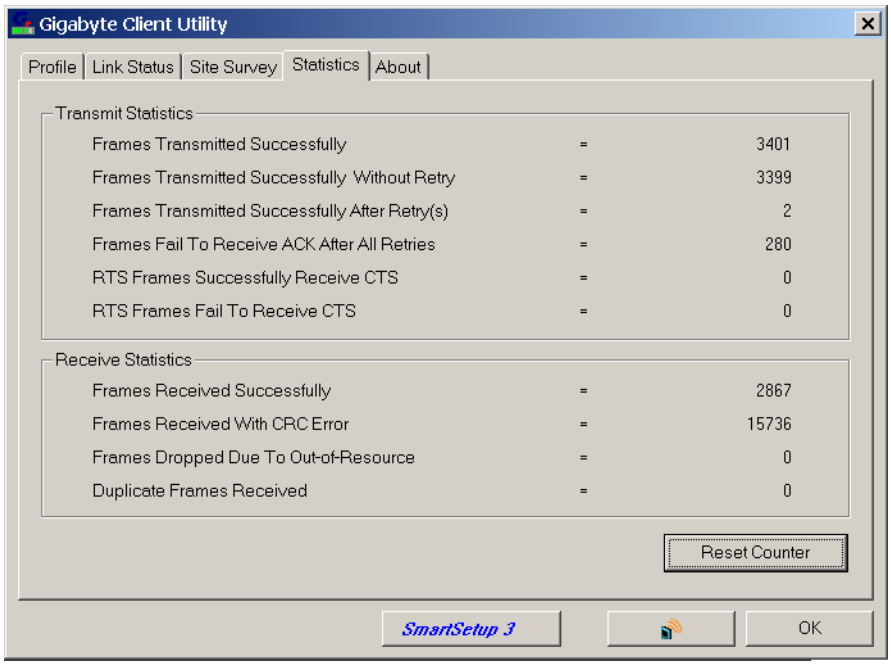
Gigabyte Client Utility
Profile
Link Status
Site Survey
Statistics
About
Transmit Statistics
Frames Transmitted Successfully = 3401
Frames Transmitted Successfully Without Retry = 3399
Frames Transmitted Successfully After Retry(s) = 2
Frames Fail To Receive ACK After All Retries = 280
RTS Frames Successfully Receive CTS = 0
RTS Frames Fail To Receive CTS = 0
Receive Statistics
Frames Received Successfully = 2867
Frames Received With CRC Error = 15736
Frames Dropped Due To Out-of-Resource = 0
Duplicate Frames Received = 0
Reset Counter
SmartSetup 3
OK

Figure 23. Statistics Tab

Description of items in ***Figure 23*** is as follows:

Frames Transmitted Successfully: Number of frames transmitted successfully.

Frames Transmitted Successfully Without Retry: Number of frames transmitted successfully, excluding packets transmitted successfully with more than one retry.

Frames Transmitted Successfully After Retry[s]: Number of frames transmitted successfully with more than one retry.

Frames Fail To Receive ACK After All Retries: Number of frames failing to receive ACK after many retries.

RTS Frames Successfully Receive CTS: Number of RTS frames successfully received CTS (Clear To Send) from AP.

RTS Frames Fail To Receive CTS: Number of RTS frames fail to receive CTS from AP.

Frames Receive Successfully: Number of frames received successfully**.**

Frames Receive With CRC Error: Number of frames received with CRC Errors.

Frames Dropped Due TO Out-of-Resource: Number of frames dropped due to out-of-resource.

Duplicate Frames Received: Number of duplicate frames received.

Reset Counter: Resets the counter to zero.

3.5. About Tab

The **About** tab displays information about current drivers and physical MAC address *(see **Figure 24**)*.

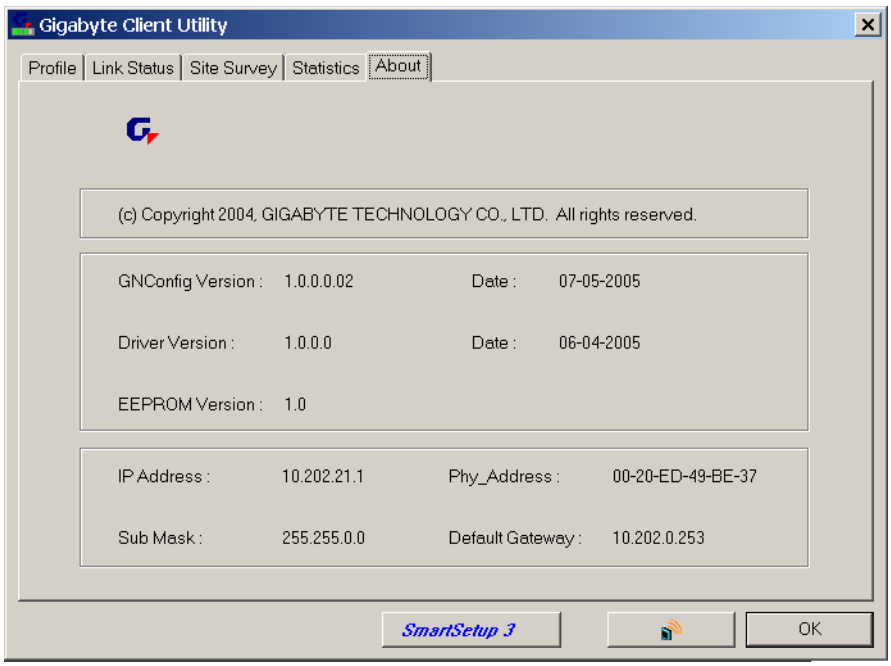

Figure 24. About Tab

GbConfig Version (Date) – The version number (and date) of the Adapter Utility

Driver Version (Date) – The version number (and date) of the Adapter Driver.

EEPROM Version - Hardware version number of the Adapter's EEPROM**.**

IP Address – The current IP Address of the Adapter.

Phy Address – The MAC address of the Adapter.

Sub Mask – The current Subnet Mask of the Adapter.

Default Gateway – The current IP Address of the Gateway (typically the IP address of the AP).

Appendix A Troubleshooting

This troubleshooting guide provides answers to some common problems which you may encounter while installing or using GIGABYTE Wireless Adapters. Contact the GIGABYTE Wireless Technical Support Team at www.giga-byte.com if you encounter problems not mentioned in this section.

Problem: Cannot connect to an AP
Advice:

- Make sure the SSID for the Wireless PCI Adapter is the same as the Access Point.
- Make sure the security settings are the same as that of Access Point. When WEP or WPA encryption is enabled, check if the WEP or WPA keys for the PCI Adapter and AP are the same.
- Make sure if the MAC address of the Adapter is added in the AP Authorization Table.

Problem: Can connect to an AP but cannot connect to the Internet
Advice:

- Make sure the security settings are the same as that of Access Point. When WEP or WPA encryption is enabled, check if the WEP or WPA keys for the PCI Adapter and AP are the same.
- Make sure the network configuration (IP address, subnet mask, gateway, and DNS) of your computer are correct.
- Check the proxy server of the WEB browser is correctly set.

Problem: Poor link quality and signal strength
Advice:

- Keep the Adapter away from microwave ovens and large metal objects to avoid radio interference.
- Keep the distance between the Adapter and the AP as close as possible.

Please check www.giga-byte.com for more complete and up to date troubleshooting tips.

Appendix B
Specifications

1. System		
Host Interface	PCI	
Chipset	Ralink MAC RT2561, Transceiver RT2527	
Operating Voltages	5.0V+/-5%	
Typical Power	Transmitting: 350mA, Receiving: 220mA	
2. RF Performance		
802.11g (backward compatible to 802.11b)		
Frequency Bands	2412 ~ 2484 MHz (subject to local regulations)	
Modulation Technology	OFDM and DSSS	
Modulation Techniques	64QAM, 16QAM, QPSK, BPSK, CCK, DQPSK, DBPSK	
Data Rates	54, 48, 36, 18,12, 9, 11, 6, 5.5, 2, and 1 Mbps, auto fallback	
Peak Output Power	Targeted at 14dBm @54Mbps, 18dBm @11Mbps	
Minimum Receive Sensitivity	Targeted at -71dBm @54Mbps; -84dBm@11Mbps	
Antenna	External antenna with the gain of 2dBi, L type	
3. Safety Regulation and Operating Environment		
EMC certification	FCC Part 15 (USA)	DGT (Taiwan)
	CE (Europe)	
Temperature Range	Operating: 0 ~ 40 degree C, Storage: -20 ~ 65 degree C	
Humidity	10% ~ 85% Non-condensing	
4. Software Support		
Driver	Windows 98SE/Me/2000/XP	
Security	64/128 bit WEP, WPA, WPA2, TKIP, 802.11i	
Quality of Service (QoS)	802.11e, WMM	
International Regulation	802.11d + h	
Cisco Compliance	CCX v1.0, v2.0, v3.0	
Roaming	Seamless roaming among 802.11b/g access points.	
Management Utility	Monitors the network situation.	
Software AP support	Yes	
5. Mechanical		
Dimensions	134mm*121mm*22mm	
Weight	50+/-5g	
Packaging	Packaging specially used by Gigabyte.	
LED indicators	Act and Link	

* Subject to change without notice.

Appendix C
Regulatory Information

CE Mark Warning: This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Europe - Declaration of Conformity

CE	This device is a 2.4 GHz low power RF device intended for home and office use in EU and EFTA member states. In some EU / EFTA member states some restrictions may apply. Please contact local spectrum management authorities for further details before putting this device into operation.

GIGA-BYTE Technology, Inc. declares that the product: **Wireless Broadband Router Model Number: GN-B49G** is in conformity with and in accordance with the European Directive of EMC, 89/336 EEC for the following sections:

EN 61000-3-2, EN 61000-3-3, EN 55024, and EN 55022 Disturbances and Immunities

GIGA-BYTE Technology, Inc. also declares the conformity of above mentioned product with the actual required safety standards in accordance with LVD Directive 73/23 EEC:

EN 60950 Safety

In accordance with R&TTE Directive 1995/5/EC, Part 17: Requirements for Operation in the European Community, GIGA-BYTE Technology, Inc declares the conformity of the above mentioned products for:

EN 300 328-2 V1.2.1, ETSI EN 300 328-1：V1.3.1, EN 301 489-1, and EN 301 489-17 Technical Requirements for Radio Equipment

Countries of Operation and Conditions of Use in the European Community
The user should run the configuration utility program provided with this product to check the current channel of operation and confirm that the device is operating in conformance with the spectrum usage rules for European Community countries as described in this section. European standards dictate a maximum radiated transmit power of 100mW EIRP and a frequency range of 2.400 - 2.4835 Ghz.

Operation using 2.4 GHz Channels in France
2.4 GHz Bande: les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) sont complétement libres d'utilisation en France (en utilisation intérieur). Pour ce qui est des autres canaux, ils peuvent être soumis à autorisation selon le department. L'utilisation en extérieur est soumis à autorisation préalable et très restreint. Vous pouvez contacter l'Autorité de Régulation des Télécommunications (http://www.art-telecom.fr) pour de plus amples renseignements.

Please check ART's web site for latest requirements for use of the 2.4GHz band in France: http://www.art-telecom.fr/eng/index.htm.
When operating in France, this device may be operated under the following conditions:
Indoors only, using any channel in the 2.4465-2.4835 GHz band.

Trademarks: GIGABYTE is a registered trademark of GIGA-BYTE Technology, Inc. Other trademarks or registered trademarks are the property of their respective manufacturers or owners.

Copyright Statement: No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation,

transformation, or adaptation without permission from GIGABYTE/GIGA-BYTE Technology, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior
notice. Copyright© 2004 by GIGA-BYTE Technology, Inc. All rights reserved.

Appendix D
Warranty

Limited Warranty Statement (1-Year Warranty)

Thank you for purchasing the GIGABYTE Product. This limited warranty statement will provide you one year warranty starting from the purchase date. Of which if any defect is occurred due to accidents or any man-made factors, or any unauthorized torn-off or damage to GIGABYTE's sticker on the product, GIGABYTE Technology will not provide after-sale services, such as:

- Products are damaged due to any violation of instructions on user manual.
- Hardware is damaged due to inappropriate assembling.
- Products are damaged due to the use of illegal accessory.
- Products are damaged due to parts disassembling without authorization.
- Products are damaged due to exceeding environment limits.
- Products are damaged due to unexpected external force.
- Products are damaged due to nature disasters.
- Products are copies or illegally smuggled goods.

PLEASE RECORD THE FOLLOWING INFORMATION REGARDING YOUR WARRANTY

Name of Customer:	
Phone No:	
Address:	
Email:	
Model:	
Serial:	
Date of Purchase:	
Place of Purchase:	
From Whom:	
Distributor:	

Customer Service

GIGA-BYTE TECHNOLOGY CO., LTD.
No.6, Bau Chiang Road, Hsin-Tien,
Taipei Hsien, Taiwan.
Tel: 886-2-8665-2665 Fax:886-2-89124007
http://www.gigabyte.com.tw